## Remarks

Claims 1-6 and 8-19 are pending in this application. By this Amendment, claims 1, 3 and 4 are amended. The Applicant cancels claim 7 without prejudice to or disclaimer of the subject matter contained therein. Reconsideration based on the above amendments and following remarks is respectfully requested.

### I. Double Patenting

The Office Action rejects claims 1-6 and 8-19 under the judicially created doctrine of obviousness-type double patenting as being unpatentable over claims 1-23 of U.S. Patent 6,530,021 to Aoki. Applicant has enclosed a Terminal Disclaimer under 37 C.F.R. §1.321(c), and a showing that Aoki and the current application are commonly owned. Accordingly, the obviousness-type double-patenting rejection is moot.

### II. Specification

The Office Action states that a substitute specification in proper idiomatic English and in compliance with 37 C.F.R. §1.52(a) and (b) is required. Applicant has provided the required substitute specification and respectfully submits that the Specification is in compliance with 37 C.F.R. §1.52(a) and (b). No new matter is added in the Substitute Specification.

### III. Claim Rejections 35 USC §112

The Office Action rejects Claim 7 under 35 U.S.C. §112, first paragraph, as failing to comply with the enablement requirement. This rejection is moot in view of the cancellation of claim 7.

Claims 1, 3, 4 and 7 under 35 U.S.C. §112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which Applicant regards as the invention. This rejection is moot in view of the cancellation of claim 7.

Regarding claim 1, line 7, the Office Action states that "group/member" lacks antecedent basis. Claim 1 was amended to delete the word "the" before "group/member."

Regarding claims 3 and 4, the Office Action states that it is unclear that whether the private key is used to decrypt the encrypted common key is the same private key, which is encrypted in being decrypted by the decrypted common key or a different key. The Office Action further asks, "why is it needed to decrypt this said encrypted private key by use of said decrypted common key to generate the said private key if that private key is already provided?" Applicant has amended claims 3 and 4 in order to clarify that a private key that corresponds to the member is used to acquire the common key, and the common key is used to acquire the private key that corresponds to the public key.

Regarding claim 4, the Office Action states that in line 14, the limitation "signature target data" lacks antecedent basis in the claim. The Applicant has amended claim 4 by inserting the word "a", in between the words "acquiring" and "signature" in line 15.

Applicant respectfully submits that claims 1, 3, and 4 are in compliance with 35 U.S.C. §112 second paragraph and respectfully requests withdrawal of the 35 U.S.C. §112 second paragraph rejection of claims 1, 3 and 4.

**IV. Claim Rejections 35 USC §102**

Claims 1-6 and 8-19 are rejected under 35 U.S.C. §102(e) over Aoki. Applicant respectfully traverses this rejection.

Regarding claim 1, the cited portions of Aoki do not disclose or teach an encrypted private key that is formed by encrypting a private key with a common key as claimed. The Office Action cites col. 8, line 17 – col. 9, line 23 and col. 10, lines 5-12. However, the cited portion of Aoki merely discloses the components of the composite lock which does not include or teach the encrypted private key as claimed.

Regarding claim 3, the cited portions of Aoki fails to teach or disclose a step for decrypting said encrypted private key included in said lock data by use of said decrypted common key to generate said private key as claimed. Specifically, the cited portion of Aoki fails to disclose the encrypted private key as claimed. The Office Action cites col. 23, line 59 – col. 24, line 3. The cited portion of Aoki merely discloses encryption by use of the common key that is encrypted with text. Although Aoki discloses creating a plurality of encrypted common keys by encrypting the common key with respective public keys of the members, the Office Action is void of any discussion in the cited portion of the reference regarding the encrypted common keys as claimed.

Regarding claim 5, Aoki fails to disclose or teach a step for encrypting said common key by use of public keys of respective group/members to generate corresponding encrypted common key. As discussed in the arguments regarding claims 1-4 above, the encrypted common key is generated by encrypting the common key by use of the public key of the respective group members. In addition, Aoki fails to disclose or teach a step for encrypting the private key by use of the common key to generate an encrypted private key as claimed. The Office Action cites col. 10, lines 1-5 and col. 12, lines 16-25. The cited portions of the reference merely disclose the composite lock list which includes a public key that is acquired from the corresponding composite lock to produce an encrypted secret key. However, this portion of the reference fails to disclose the encrypted private key as claimed, nor does it disclose the encrypted common key as claimed.

Regarding claim 6, the rejection of this claim is respectfully traversed at least for the same arguments as those given regarding claims 1-5. Although Aoki discloses the step for modifying the private key by use of a desired function, including an inverse function, to generate a modified private key, the recited portion fails to disclose encrypting the modified

private key by use of the common key to generate an encrypted modified private key as claimed.

Regarding claim 8, the Office Action asserts that the lock data further includes a public key for verifying a signature, an encrypted signature private key which is formed by encrypting a signature private key for writing said signature by use of a public key of a changing right holder, and a signature written by use of said signature private key on desired data included in said lock data. The Office Action cites col. 1, lines 47-50, col. 4, lines 42-46, and col. 18, lines 13-35. However, since claim 8 depends from claim 5, it would be allowable at least for the same reasons stated for claim 5.

Regarding claim 9, the Applicant respectfully traverses this rejection at least on the same grounds as discussed for claims 1-5 above. Specifically, Aoki fails to disclose or teach the encrypting of a private key corresponding to the first public key by use of a common key as claimed. The Office Action asserts that Aoki discloses a second private key for verifying a signature, an encrypted signature private key formed by encrypting a signature private key for writing said signature by use of a public key of a changing right holder, said first public key, said encrypted private key, said encrypted common key, said second public key, and a signature written by use of said signature private key on said encrypted signature private key. The Office Action cites col. 9, lines 14-23, col. 13, lines 36-47, col. 13, lines 54-60, and col. 14, lines 17-15. The cited portions of Aoki disclose the public key of a change lock, the public key of a group lock, a group secret key that has directly or indirectly been encrypted an individual secret key, and a public key that is used to change the group lock. However, the cited portions of Aoki fail to disclose or teach an encrypted private key formed by encrypting a private key, corresponding to the first public key, by use of a common key as claimed.

Regarding claims 10, 11, 12 and 13, since claims 10, 11, 12 and 13 depend from claim 9, claims 10, 11, 12 and 13 are allowable at least for the same reasons as claim 9.

Regarding claims 16-19, the Office Action states that the rejection is applied to like elements concerning claims 1-5 above. The Office Action cites col. 3, lines 20-50. Applicant respectfully traverses these rejections. Applicant respectfully asserts that the cited portion of the reference fails to disclose or teach encrypting a private key corresponding to said public key, by use of a common key as claimed.

Applicant respectfully submits that Aoki fails to teach or disclose all of the features recited in claims 1-6 and 8-19.

Accordingly Aoki fails to anticipate the subject matter of claims 1-6 and 8-19 under 35 U.S.C. §102(e). Withdrawal of the rejection of claims 1-6 and 8-19 under 35 U.S.C. §102(e) as unpatentable over Aoki is respectfully requested.

**V. Claim Rejection 35 USC §103**

Claim 7 is rejected under 35 U.S.C. §103(a) over Aoki in view of U.S. Patent 5,852,665 to Gressel et al. This rejection is moot in view of the cancellation of claim 7.

**VI. Conclusion**

In view of the foregoing, Applicant respectfully submits that this application is in condition for allowance. Favorable reconsideration and prompt allowance of claims 1-6 and 8-19 are earnestly solicited.

Should the Examiner believe that anything further would be desirable in order to place this application in even better condition for allowance, the Examiner is invited to contact Applicant's undersigned representatives at the telephone number listed below.

Respectfully submitted,

James A. Oliff
Registration No. 27,075

David E. Brown
Registration No. 51,091

deb

PROPOSED

Date: [illegible]

**OLIFF & BERRIDGE, PLC**
**P.O. Box 19928**
**Alexandria, Virginia 22320**
**Telephone: (703) 836-6400**

DEPOSIT ACCOUNT USE AUTHORIZATION
Please grant any extension necessary for entry;
Charge any fee due to our Deposit Account No. 15-0461